



UNITED STATES PATENT AND TRADEMARK OFFICE

A
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/871,084	05/30/2001	Frederick D. Weber	TT3763	2031
23720	7590	09/13/2005	EXAMINER	
WILLIAMS, MORGAN & AMERSON, P.C. 10333 RICHMOND, SUITE 1100 HOUSTON, TX 77042			ZAND, KAMBIZ	
			ART UNIT	PAPER NUMBER
			2132	
DATE MAILED: 09/13/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/871,084	WEBER ET AL.
	Examiner	Art Unit
	Kambiz Zand	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 26 July 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 30-57 and 63-70 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 30-39, 44-53, 57, 63-66, 68 and 70 is/are rejected.
- 7) Claim(s) 40-43, 54, 56, 67 and 69 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 01 June 2001 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35, U.S. Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1-29, 58-62 have been withdrawn with traverse, **however the applicant have not provided no arguments in that regard in the response filed on 07/26/2005**. Therefore Reply to Final Must include Cancellation as set forth below:

This application contains claims 1-29 and 58-62 drawn to an invention nonelected with traverse in Paper No. 20050505. **A complete reply to the final rejection must include cancellation of nonelected claims or other appropriate action (37 CFR 1.144). See MPEP § 821.01.**

4. Claims 45, 46, 55 and 68 have been amended.
5. Claims 30-57 and 63-70 are pending.
6. Examiner withdraws rejection of claims 45, 46, 55 and 68 under 35 U.S.C 112-second paragraphs due to correction by the applicant.
7. Examiner withdraws double patenting rejection of claims 30, 50 and 63 due to approval of terminal disclaimer filed on 07/26/2005 by applicant.

Response to Arguments

8. Applicant's arguments filed 07/26/2005 have been fully considered but they are not persuasive.

As per applicant's arguments with respect to claims 30 and 45 that **Takahashi** does not describe or suggest "security hardware that includes a lock override register configured to deny access to one or more secure assets when a lock override it is set"; restricting access to the security assets in response to the computer system being in a first operating mode that is different from a secure operating mode"; and "requesting access to the security assets while in the first operating mode, and permitting access to the security assets in response to receiving access to the secured assets while in the first operating mode" with respect to claims 50 and 63, examiner makes the following remarks:

- Applicant's lock override registers corresponds to the ROM 24 and where the override setting corresponds to the action of the pointer 51 to set the mode and the function to be implemented. Security hardware corresponds to assurance logic 27, crypto I/O 25 that works with the other elements of the system.
- See abstract where the internal operating system only deals with general access and the access to cryptography functions are prohibited since that

type of the function are done by secure mode (see also col.2, lines 48-67 and col.3, lines 1-15).

As per applicant's arguments with respect to claims 30 and 45 that Angelo does not describe or suggest "security hardware that includes a lock override register configured to deny access to one or more secure assets when a lock override it is set"; restricting access to the security assets in response to the computer system being in a first operating mode that is different from a secure operating mode"; and "requesting access to the security assets while in the first operating mode, and permitting access to the security assets in response to receiving access to the secured assets while in the first operating mode" with respect to claims 50 and 63, examiner makes the following remarks:

- Angelo et al. teach method for securely managing encryption information in a computer system, having a secure mode of operation and a normal mode of operation" (col 10 lines. 53-55) which read on the limitation "a processor configured to operate in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode". The limitation "one or more secured assets coupled to the processor" is met by secure memory (col. 3 lines 12-16). Furthermore, Angelo et al. teach storing an encryption algorithm in a secure memory space not accessible to the normal software processes and only

accessible by the general processor in the secure mode of operation" (col 10 line 66- col. 11 line 2) and PCI-ISA bridge to allow access to protected resources (col. 4 lines 56- 649. This reads on security hardware configured to control access to the secured assets dependant upon the operating mode of the processor, wherein the security hardware is configured to allow access to the secure assets in the secure operating mode".

Claim Objections

9. **Claim 43** is objected to because of the following informalities: typo error.

Examiner suggests the following corrections:

- In claim 43 the "in lieu of data" phrases makes the claim unclear in that neither means nor interrelationship of means are set forth in these claims in order to achieve the desired results expressed in the "in lieu data" phrases. The phrase is a confusing term since any response contains data. Corrections or clarification is requested. If Applicant traversing the rejection, then the clarification should be specific to which embodiment of the invention such phrase is related and where in the specification it has such support.

Claim Rejections - 35 USC § 102

10. Claims 30, 45, 50 and 63 are rejected under 35 U.S.C. 102(b) as being anticipated by Takahashi et al. (U.S. Patent No. 56152633).

As per claim 30, 50 and 63 Takahashi et al. teach "A secure mode within a dual mode processor

is implemented" (Abstract) reads on claim 30 wherein a processor is configured to operate in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode.

Takahashi et al. teach primitives which encrypt/decrypt the data (secure assets), I/O hardware control circuit and assurance logic (security hardware) (col.2 lines 10-13, col. 3 lines 53-59 and col. 4 lines 29-34) which read on "security hardware configured to control access to the secured assets dependant upon the operating mode of the processor, wherein the security hardware is configured to allow access to the secure assets in the secure operating mode".

As per claim 45 Takahashi et al. teach that in while in secure mode, processing functions execute only the secure primitives in ROM but they still have the ability to access external memory for data (col.3 lines 53-57), which reads on the processor being configured to store and retrieve data from the memory in all of

the plurality of operating modes.

11. claims 30, 32-38, 48, 50 and 63 are rejected under 35 U.S.C. 102(e) as being anticipated by Angelo et al. (U.S. Patent No. 6581 162).

As per claim 30, 50 and 63 Angelo et al. teach method for securely managing encryption information in a computer system, having a secure mode of operation and a normal mode of operation" (col 10 lines. 53-55) which read on the limitation "a processor configured to operate in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode".

The limitation "one or more secured assets coupled to the processor" is met by secure memory (col. 3 lines 12-16).

Furthermore, Angelo et al. teach storing an encryption algorithm in a secure memory space not accessible to the normal software processes and only accessible by the general processor in the secure mode of operation" (col 10 line 66- col. 11 line 2) and PCI-ISA bridge to allow access to protected resources (col. 4 lines 56- 649. This reads on security hardware configured to control access to the secured assets dependant upon the operating mode of the processor, wherein the security hardware is configured to allow access to the secure assets in the secure operating mode"

As per claim 32-33 Angelo et al. teach system management mode

(SMM) which is entered upon receipt of a system management interrupt (SMY).

Angelo et al. also teach SMI asserted by either an SMI timer or by a system request upon which the entire CPI state is saved in the SMM memory. After the initial processor state is saved, the processor begins executing an SMI handler routine providing security services (col 7 line 43- col. 8 line 43).

The above reads on receiving a request to change the computer system from the first operating mode to the secure operating mode, providing an entry into an initiation register and accessing the control signal indicative of the entry providing a system management interrupts.

As per claims 34-38 Angelo et al. teach timers (col. 4 line 58). When the computer system detects a request for secure communications or any event requiring secure entry of encryption information. Control then proceeds to step where appropriate registers in processor are loaded prior to execution of the SMI code (Fig. 5, col. 9 lines 3-13). The computer systems don't wait indefinitely for input of the sensitive information like passwords. Timer measuring a time period in which the computer system is in the secure operating mode, and providing a control signal to exit the secure mode in response to the time period in which the computer system is in the secure operating mode exceeding a predetermined length of time are used complete indefinite sessions.

As per claim 48 Angelo et al. teach a battery providing reserve power to the security hardware (col. 8 lines 23-25).

12. All other claims limitations excluding the allowable subject matters below are taught by the above references either single or in combination. Please see the entire references.

Allowable Subject Matter

13. Claims 40-43, 54, 56, 67 and 69 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and

Art Unit: 2132

any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally be reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Kambiz Zand

09/09/2005

AU2132